

AMENDMENTS TO THE CLAIMS

Claim 1. (Currently amended) A key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a suppliable number, which is a number showing how many indicating a number of times the decryption key can be supplied, with respect to a terminal apparatus connected to a network, the key delivery apparatus comprising:

a receiving unit operable to receive, from the terminal apparatus, a supply request, which is a request for the decryption key;

a supply determining judging unit operable, if the terminal apparatus is a legitimate supply target, to judge determine whether the terminal apparatus is one a terminal apparatus of a first-type terminal apparatus that manages a content-usage period, and whether the terminal apparatus is a terminal apparatus of a second-type terminal apparatus that does not manage the content-usage period; and

a key supply unit operable, if the suppliable number has indicates a remaining number that the decryption key can be supplied, to supply to the terminal apparatus, (i) the decryption key and a key-usage period of the decryption key when judged if the supply determining unit determines that the terminal apparatus is the of the first-type terminal apparatus, and (ii) the decryption key when judged, without the key-usage period, if the supply determining unit determines that the terminal apparatus is of the second-type terminal apparatus, wherein

the supply determining judging unit judges determines that the terminal apparatus to be is of the first-type terminal apparatus if the terminal apparatus records the encrypted content, the decryption key, and the key-usage period onto a portable recording medium.

Claim 2. (Currently amended) The key delivery apparatus of claim 1, wherein:

the network is a home network connected to an external network[[],];

contents are content is received from outside the home network[[],]; and

the key delivery apparatus judges determines whether each terminal apparatus terminal apparatuses connected to the home network to be is a legitimate supply targets target.

Claim 3. (Currently amended) The key delivery apparatus of claim 1, further comprising:

a key-information storage unit operable to store the key-usage period subsequent to ~~supply of the key supply unit supplying the decryption key and the key-usage period to the terminal apparatus of the first-type terminal apparatus;~~

a period determining judging unit operable to judge determine whether the key-usage period has expired; and

a time management unit operable to add “1” to the suppliable number when ~~judged the period determining unit determines~~ that the key-usage period has expired.

Claim 4. (Currently amended) The key delivery apparatus of claim 3, further comprising:

a date-time storage unit operable to store at least one of a first ~~group-grouping~~ and a second ~~grouping group~~, the first ~~group including-grouping formed from~~ (i) date-time information ~~showing indicating~~ the key-usage period and a supply date-time of the decryption key, and (ii) identification information ~~showing the indicating the~~ supply target to be ~~the terminal apparatus of the first-type terminal apparatus~~, and the second ~~group including-grouping formed from~~ (i) date-time information ~~showing a indicating the~~ supply date-time of the decryption key, and (ii) identification information ~~showing indicating the supply target to be the terminal apparatus of the second-type terminal apparatus~~;

a date-time determining judging unit operable to judge determine whether a present date-time has reached the supply date-time; and

a date-time supply unit operable, when ~~judged the data time determining unit determines~~ that the present date-time has reached the supply date-time, to supply the decryption key and the key-usage period to ~~the terminal apparatus of the first-type terminal apparatus or supply the decryption key to the terminal apparatus of the second-type terminal apparatus~~, based on the identification information.

Claim 5. (Currently amended)

The key delivery apparatus of claim 4, further comprising:

a search requesting unit operable to transmit, to the terminal apparatus of the first-type terminal apparatus and the terminal apparatus of the second-type terminal apparatus, search information showing identifying the decryption key; and

a proprietary information receiving unit operable to receive information indicating whether that the decryption key is stored by being held, from whichever of the terminal apparatus of the first-type terminal apparatus and or the terminal apparatus of the second-type terminal apparatus holds the decryption key.

Claim 6. (Currently amended)

The key delivery apparatus of claim 5, wherein:

the key delivery apparatus stores secret information, which is information to be used as a reference when determining used as a reference in judging whether the terminal apparatus is-a the legitimate supply target[[],];

the supply determining judging unit includes an authentication subunit operable to judge determine whether the terminal apparatus holds is storing the secret information[[],]; and

the supply determining judging unit judges determines that the terminal apparatus to be a is the legitimate supply target when judged the supply determining unit determines that the terminal apparatus holds is storing the secret information.

Claim 7. (Currently amended)

The key delivery apparatus of claim 6, wherein:

the key supply unit includes a remaining number determining judging subunit operable to judge determine whether the suppliable number is greater than a predetermined reference number[[],]; and

the key supply unit judges determines that the suppliable number to have indicates the remaining number that the decryption key can be supplied when judged the key supply unit determines that the suppliable number is greater than the predetermined reference number.

Claim 8. (Currently amended)

The key delivery apparatus of claim 7, wherein:

the key supply unit further includes an encryption subunit operable (i) to encrypt the decryption key and the key-usage period when the decryption key and the key-usage period are to be supplied to the terminal apparatus of the first-type terminal apparatus; and (ii) to encrypt the decryption key when the decryption key is to be supplied to the terminal apparatus of the second-type terminal apparatus; and

the key supply unit, when judged the key supply unit determines that the suppliable number has indicates the remaining number that the decryption key can be supplied, supplies supplies to the terminal apparatus, (i) the encrypted decryption key and the encrypted key-usage period when judged it is determined that the terminal apparatus is of the first-type terminal apparatus and (ii) the encrypted decryption key when judged it is determined that the terminal apparatus is of the second-type terminal apparatus.

Claim 9. (Currently amended)

The key delivery apparatus of claim 8, further comprising:

a historical information storage unit operable to store historical information showing indicating a connection date-time of the terminal apparatus of the first-type terminal apparatus;

a connection determining judging unit operable to judge determine, using the connection date-time, whether the terminal apparatus of the first-type terminal apparatus was connected to the network within a predetermined connection period; and

a connection management unit operable to add “1” to the suppliable number when judged it is determined that the terminal apparatus of the first-type terminal apparatus was not connected to the network within the predetermined connection period.

Claim 10. (Currently amended)

The key delivery apparatus of claim 8, further comprising:

a frequency storage unit operable to store a usage frequency of the decryption key by the terminal apparatus of the first-type terminal apparatus;

a frequency determining judging unit operable to judge determine whether the usage frequency has reached a predetermined reference frequency; and

a connection management unit operable to add “1” to the suppliable number when judged it is determined that the usage frequency has reached the predetermined reference frequency.

Claims 11-16. (Canceled)

Claim 17. (Currently amended) A portable recording medium that receives a supply of a decryption key, for decrypting an encrypted content, from a key delivery apparatus that manages the decryption key, the portable recording medium comprising:

a key reception unit operable to receive the decryption key and a key-usage period of the decryption key from the key delivery apparatus, when judged in the key delivery apparatus determines that supply of supplying the decryption key to the portable recording medium is possible; and

a key-information storage unit operable to store the decryption key and the key-usage period[.];

a period determining unit operable to determine whether the key-usage period has expired; and

a deletion unit operable to delete the decryption key and the key-usage period when the period determining unit determines that the key-usage period has expired.

Claim 18. (Currently amended) The recording medium of claim 17, wherein the key reception unit includes a decryption subunit operable, when the decryption key and the key-usage period of the decryption key are to be received, to (i) receive an encrypted decryption key and an encrypted key-usage period, and to (ii) decrypt the encrypted decryption key and decrypt the encrypted key-usage period, and to (iii) generate the decryption key and the key-usage period.

Claim 19. (Canceled)

Claim 20. (Currently amended) The recording medium of claim 17, further comprising:

a proprietary determining-judging unit operable to receive, from the key delivery apparatus, search information showing identifying the decryption key, and operable to judge determine whether the decryption key is held in stored on the portable recording medium, using the search information; and

a proprietary notifying unit operable, when judged the proprietary determining unit determines that the decryption key is held in stored on the portable recording medium, to notify transmit, to the key delivery apparatus, information indicating that the decryption key is held in stored on the recording medium.

Claim 21. (Currently amended) A key delivery system comprising:

- (i) a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a suppliable number, which is a number showing how many indicating a number of times the decryption key is suppliable can be supplied, with respect to a terminal apparatus connected to a network;
- (ii) a first-type terminal apparatus that manages a content-usage period; and
- (iii) a second-type terminal apparatus that does not manage the content-usage period,

wherein:

the key management delivery apparatus including includes:

- a receiving unit operable to receive, from the terminal apparatus, a supply request, which is a request for the decryption key;
- a supply determining-judging unit operable, if the terminal apparatus is a legitimate supply target, to judge determine whether the terminal apparatus is one of a terminal apparatus of the first-type terminal apparatus and whether the terminal apparatus is a terminal apparatus of the second-type terminal apparatus; and
- a key supply unit operable, if the suppliable number indicates has a remaining number that the decryption key can be supplied, to supply to the terminal apparatus, (i) the decryption key and a key-usage period of the decryption key when judged if the supply determining unit determines that the terminal apparatus is of the first-type terminal apparatus and (ii) the decryption key when judged, without the key-usage period, if the supply determining unit determines that the terminal apparatus is the second-type terminal apparatus; wherein

_____ the supply determining judging unit judges determines that the terminal apparatus ~~to be~~ is of the first-type terminal apparatus if the terminal apparatus records the encrypted content, the decryption key, and the key-usage period onto a portable recording medium[[,]];:

_____ the first-type terminal apparatus receives, from the key delivery apparatus, and stores store the decryption key and the key-usage period[[,]]; and

_____ the second-type terminal apparatus receives the decryption key from the key delivery apparatus, and uses use the decryption key for-in content usage.

Claim 22. (Currently amended) A key supply method used of using-in a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a suppliable number, which is a number indicating showing how many a number of times the decryption key is suppliable can be supplied, with respect to a terminal apparatus connected to a network, the key supply method comprising the steps of:

receiving, from the terminal apparatus, a supply request, which is a request for the decryption key;

determining, judging, if the terminal apparatus is a legitimate supply target, whether the terminal apparatus is ~~one~~ a terminal apparatus of a first-type terminal apparatus that manages a content-usage period and whether the terminal apparatus is a terminal apparatus of a second-type terminal apparatus that does not manage the content-usage period; and

supplying to the terminal apparatus, if the suppliable number has indicates—a remaining number that the decryption key can be supplied, (i) the decryption key and a key-usage period of the decryption key when judged if the determining determines that the terminal apparatus is of the first-type, terminal apparatus and (ii) the decryption key when judged, without the key-usage period, if the determining determines that the terminal apparatus is of the second-type terminal apparatus.

Claim 23. (Canceled)

Claim 24. (Currently amended) A computer-readable recording medium storing a key supply computer program used ~~in~~ by a key delivery apparatus that manages a decryption key for decrypting an encrypted content and manages a suppliable number, ~~which is a number showing how many~~ indicating a number of times the decryption key ~~is~~ can be supplied, with respect to a terminal apparatus connected to a network, the key supply computer program comprising the steps of: ~~causing the key delivery apparatus to execute a method comprising:~~

receiving, from the terminal apparatus, a supply request ~~which is a request~~ for the decryption key;

~~determining~~ judging, if the terminal apparatus is a legitimate supply target, whether the terminal apparatus is ~~one of~~ a terminal apparatus of a first-type terminal apparatus that manages a content-usage period and ~~whether the terminal apparatus is a~~ terminal apparatus of a second-type terminal apparatus that does not manage the content-usage period; and

supplying to the terminal apparatus, if the suppliable number ~~has~~ indicates a remaining number ~~that the decryption key can be supplied~~, (i) the decryption key and a key-usage period of the decryption key ~~when judged~~ if the determining determines that the terminal apparatus is ~~of~~ the first-type, terminal apparatus and (ii) the decryption key ~~when judged, without the key-usage period~~, if the determining determines that the terminal apparatus is ~~of~~ the second-type terminal apparatus.